

IN THE CLAIMS

1 (Previously Presented). A method comprising:
identifying a firmware upgrade request by a firmware program;
retrieving a file signed with a private key;
validating the file with a public key;
upgrading a portion of the firmware program by the firmware program;
locking a device storing the firmware program such that a second portion of the
firmware program is not readable;
validating the public key; and
retrieving a second public key from the firmware program if the public key is not
valid.

Claim 2 (Canceled).

3 (Original). The method of claim 1, identifying a firmware upgrade request by a
firmware program further comprising:
reading a flag, wherein the flag is located in a non-volatile medium; and
determining that the flag is set.

4 (Original). The method of claim 3, further comprising:
deleting the file; and
clearing the flag.

5 (Original). The method of claim 1, further comprising:
determining that the file is not authentic; and
locking the device.

6 (Original). The method of claim 1, further comprising:
locking the device after upgrading a portion of the firmware program by the
firmware program.

7 (Original). The method of claim 1, wherein the second portion of the firmware program is a public key.

Claims 8-12 (Canceled).

13 (Previously Presented). A system comprising:

- a file signed by a private key;
- a device for storing a program, wherein the device may lock access to the program;

and

- a firmware program stored in the device, which, upon execution:
 - determines that an upgrade flag is set;
 - retrieves the file;
 - validates the file using a public key;
 - upgrades a first portion of the firmware program;
 - locks the device such that the a portion of the firmware program is not

readable;

- said firmware program including a second portion including:
 - a minimal boot portion;
 - a signature authentication portion; and
 - a write device portion;
- said firmware program first portion including:
 - the public key; and
 - a backup public key.

Claim 14 (Canceled).

15 (Original). The system of claim 13, wherein the firmware program further clears the upgrade flag.

16 (Original). The system of claim 13, further comprising:

- a persistent storage, wherein the file is located in the persistent storage.

17 (Original). The system of claim 13, further comprising:
a network interface for connecting the system to a network, wherein the file is retrieved from the network.

Claim 18 (Canceled).

19 (Original). The system of claim 13, wherein the portion of the firmware program further comprises:

- a hardware initialization portion;
- an operating system loader portion; and
- a device lock-out portion.

Claim 20 (Canceled).

21 (Original). The system of claim 13, wherein the device is a flash memory.

Claims 22-26 (Canceled).

27 (Previously Presented). An article comprising a medium storing instructions for enabling a processor-based system to:

- identify a firmware upgrade request by a firmware program;
- retrieve a file signed with a private key;
- validate the file with a public key;
- upgrade a portion of the firmware program by the firmware program;
- lock a device storing the firmware program such that the public key is not readable;
- validate the public key; and
- retrieve a second public key from the firmware program if the public key is not valid.

Claim 28 (Canceled).

29 (Previously Presented). The article of claim 27, further storing instructions that enable the processor-based system to:

- determine that the file is not authentic; and
- lock the device.

Claims 30 and 31 (Canceled).

32 (Previously Presented). A method comprising:

- identifying a firmware upgrade request by a firmware program;
- retrieving a file signed with a private key;
- validating the file with a public key;
- upgrading a portion of the firmware program by the firmware program; and
- locking a device storing the firmware program such that a second portion of the firmware program is not readable;
- validating the public key;
- retrieving a second public key from the firmware program if the public key is not valid;
- reading a flag, wherein the flag is located in a non-volatile medium;
- determining that the flag is set;
- deleting the file; and
- clearing the flag.

33 (Previously Presented). A method comprising:

- providing a first portion of a firmware code which is not upgradable;
- providing a second portion of a firmware code that is upgradable; and
- providing information for authenticating an upgrade of the second portion in the first portion.

34 (Previously Presented). The method of claim 33 including locking the first portion to prevent reading said first portion.

35 (Previously Presented). The method of claim 31 including providing a signature authentication in said first portion.

36 (Previously Presented). The method of claim 34 including providing two public keys.

37 (Previously Presented). The method of claim 36 including providing two identical public keys.

38 (Previously Presented). The method of claim 34 including providing instructions in said first portion to confirm the validity of a firmware upgrade file.

39 (Previously Presented). The method of claim 34 including determining whether an upgrade request is authentic and if said upgrade request is not authentic, locking the first portion against being written.

40 (Previously Presented). A processor-based system comprising:
a processor; and
a storage storing a basic input/output system, said basic input/output system including a first portion that is not upgradable and a second portion that is upgradable, said first portion including an upgrade verification code.

41 (Previously Presented). The system of claim 40 including a public key in said first portion.

42 (Previously Presented). The system of claim 40 including two public keys in said first portion.